2010



BSA GLOBAL CYBERSECURITY FRAMEWORK



BSA GLOBAL CYBERSECURITY FRAMEWORK

Over the last 20 years, consumers, businesses and governments¹ around the world have moved online to conduct business, and access and share information. This shift to a digital world has revolutionized personal interactions, education, commerce, government, healthcare, communications, science, entertainment and the arts, etc. It has delivered unprecedented efficiencies, and it will continue to yield immense benefits to our global society.

However, as opportunities expand, so do the number of risks. Consumers, businesses and governments face a variety of online threats, which can undermine trust in the digital environment – the single greatest platform for commerce and sharing information.

Protecting cyberspace is a shared responsibility. No single entity or group of stakeholders can address the problem alone – and no individual or group is without responsibility for playing a part in cybersecurity. The technology industry, consumers, businesses and governments must all take steps to secure their own systems and to collaborate with each other to define and implement comprehensive cybersecurity policies and technologies.

Cybersecurity is not just about protecting against current threats. It also yields the benefit of enabling greater and more sophisticated uses of the digital environment. Cybersecurity gives individuals, companies and governments greater confidence that they can operate in this environment and can entrust it with valuable assets and information.

Governments around the world have a multifaceted role to play in cybersecurity, including:

- Protecting their information systems.
- Working with the private sector to protect the digital infrastructure.
- Investigating, pursuing and prosecuting cybercriminals.

Currently, too few governments are sufficiently policing cyberspace, and few have put in place needed policies to effectively contribute to global cybersecurity. Significant opportunities exist to work globally and collaboratively to improve cybersecurity.

No country can address cybersecurity risks in isolation. The Business Software Alliance (BSA) Global Cybersecurity Framework is a comprehensive roadmap to build an integrated and functioning global policy response to cybersecurity.

¹ For the purposes of this document, the term "governments" includes the European Union institutions.



Guiding Cybersecurity Principles

To help governments build and implement comprehensive and workable plans that function at the national and global levels, BSA has established the following set of guiding principles:

- **Trust**—cybersecurity policy should enhance the confidence of consumers, businesses and governments in the confidentiality, integrity and availability of the online environment.
- Innovation—cybersecurity is a fast-paced race, in which we must stay ahead of cybercriminals who adapt constantly. Cybersecurity policy should maximize the ability of organizations to develop and adopt the widest possible choice of cutting edge cybersecurity solutions.
- A risk-based approach—consumers, businesses and government agencies seek to protect a wide spectrum of targets against a wide variety of cyber threats. Cybersecurity policy should enable them to implement the security measures that are most appropriate to mitigating the specific risks they face.
- International standards—industry-led, internationally accepted standards² underpin the global information technology (IT) ecosystem and spur the development and use of innovative and secure technologies. Cybersecurity policy should preserve the role of international standards.
- **Global policy convergence**—cybersecurity policy must recognize the borderless nature of the Internet, of the global economy and of cyber threats. As a result, governments should cooperate to ensure their national cybersecurity policy frameworks integrate with global approaches and practices.

A 12-Point Roadmap for Global Cybersecurity

To help governments implement the guiding principles listed above, BSA has developed a specific 12-point roadmap to guide policy and enforcement efforts. This roadmap is focused on helping governments develop strong, workable policies to improve cybersecurity at a national level, while at the same time contributing to, and integrating with, an international framework for global cybersecurity. This roadmap includes the following key efforts.

Deter and punish cybercrime

- 1. Governments should enact strong laws against cybercrime:
 - Ratify, and adopt laws to implement, the Council of Europe Cybercrime Convention.
 - Countries that are not ready or able to ratify the Convention should look to alternative resources, such as BSA's model cybercrime law, to modernize and harmonize their domestic laws.

- 2. It is publicly available without cost or for a reasonable fee to any interested party;
- 3. Any patent rights necessary to implement the standard are available to all implementers on reasonable and non-discriminatory (RAND) terms, either with or without payment of a reasonable royalty or fee; and
- 4. It should be in sufficient detail to enable a complete understanding of its scope and purpose and to enable competing implementations by multiple vendors.

² For the purposes of this document, the term "standards" means a specification with the following characteristics:

^{1.} It is developed through an open, consensus-based process;



- Laws need to be regularly updated to address all aspects of modern cybercriminal activity.
- Laws need to provide deterrent criminal penalties and civil damages.
- Governments need to make fighting cybercrime a priority by efficiently and effectively <u>enforcing cybercrime laws</u>, including allocating adequate resources to enforce cybercrime laws:
 - Sufficient numbers of dedicated investigators, prosecutors and judges.
 - Law enforcement personnel need to be trained about sophisticated cybercrime.
 - Law enforcement also needs adequate equipment to conduct investigations.
- 3. Cybercrime rings often span the globe. <u>Law enforcement action must also take place across</u> <u>borders</u>:
 - Law enforcement agencies need to build networks of relationships with their counterparts in other countries and regions.

Adopt a risk-based approach to cyber threats

Consumers, businesses and government agencies seek to protect a wide spectrum of targets against a wide variety of cyber threats. A fundamental principle of effective security protection is that not all targets require the same level of protection, and not all threats present the same risk. Cybersecurity policy should therefore enable consumers, businesses and government agencies to implement the security measures that are most appropriate to mitigating the specific risk they face.

- 4. Governments should preserve the contribution of industry-led, internationally accepted standards to global cybersecurity:
 - These standards not only underpin the global IT ecosystem, but they greatly contribute to cybersecurity by spurring the development and use of innovative and secure technologies.
 - Governments should permit the use of cybersecurity technologies according to internationally accepted, private sector developed standards, and the use of various solutions and approaches to cybersecurity.
 - Governments should not mandate compliance with country-specific cybersecurity standards, in particular standards developed by government agencies. Such mandates may cut off their country's access to the most innovative, cost-effective and valuable security technologies offered on the global marketplace, as well as inhibit their domestic industry from competing on equal terms with their foreign competitors. For example, governments should not require or mandate proprietary cryptographic algorithms or artificially limit the strength of encryption, but should accept publicly available, peerreviewed algorithms.
- 5. Governments should maintain a policy of <u>technology neutrality</u> when they develop cybersecurity policies and laws:
 - Governments should not prohibit or require the acquisition or deployment of specific products or technologies, including specific hardware or software.
 - Technology-neutral policies are fundamental to effective cybersecurity protection because they ensure that individuals and organizations can deploy the security measures that are necessary to mitigate the specific cyber risks they face.



- 6. <u>Governments should lead by example in implementing risk-based security</u> measures (people, process and technology) to protect their computers, networks and systems.
- 7. Governments should partner with industry to develop strategies to strengthen cybersecurity and privacy through improved use of reliable and risk-based online identity management, authentication and access control solutions:
 - Unreliable identity, authentication and access controls are one of the major factors facilitating successful cyber attacks.
 - Any strategy to improve the use of reliable electronic identities must respect privacy.
 - Greater use of identity, authentication and access controls solutions that offer levels of protection commensurate with risk would protect privacy and foster cybersecurity.

Inform and protect consumers

- 8. Governments need to <u>educate the public</u> home users, children and small businesses in particular about "cyber hygiene," "safe" and "ethical" computing:
 - This includes education about software piracy, because many risks to the public come from the use of pirated software.
 - Governments should tap industry resources for such efforts because industry and the IT industry in particular – have developed a great deal of educational cybersecurity material, have marketing expertise and have established channels to communicate with the public.
- 9. If governments are considering whether they should create legal frameworks about data protection and privacy, they should consider whether requirements would be appropriate to <u>protect personally identifiable information against unauthorized access and disclosure</u>. Such data security frameworks should take inspiration from existing best practices, such as:
 - How public and private organizations develop, implement, maintain and enforce administrative, technical and physical safeguards of personally identifiable information.
 - If such requirements are instituted, they should be reasonable and appropriate to the size and complexity of the entity, the nature and scope of its activities and proportional to the likelihood and severity of the potential harm.
- 10. If governments are considering whether they should create legal frameworks to require that public and private organizations <u>notify security breaches of sensitive consumer data</u>, they should consider the following recommendations based on existing best practices:
 - Limit such breach notification requirements to situations where there is a significant risk of personally identifiable information being used to cause harm.
 - Provide that notification is not required if the PII has been rendered unusable, unreadable or indecipherable to an unauthorized third party through the use of practices or methods such as encryption, redaction, access controls and other such mechanisms which are widely accepted as effective industry practices or industry standards.
 - Provide for government enforcement and preclude liability to third parties.
 - Be flexible enough to take into account the great variety of business arrangements as well as the risks confronted within specific industry or market segments.



Build capacity to prevent and respond to cyber incidents

- 11. Governments should build capacity to facilitate <u>the sharing of cybersecurity information</u> among companies and between the government and private sector (e.g. actionable threat information, response plans, etc.) Information sharing can enhance the protection of critical information infrastructure, most of which is owned and operated by the private sector:
 - Governments should facilitate this information sharing by supporting the creation of public, private and joint capabilities. This includes both human and technical resources, as well as appropriate legal protections against anti-trust claims, disclosure requirements, etc.
 - Governments should promote the development and adoption of industry best practices on information sharing.
 - Governments should address any policy or legal barriers that may inhibit information sharing. However, information sharing must be voluntary. Any obligation to share data would run against the need for organizations to comply with incompatible legal requirements (such as privacy laws, wherever they are applicable), and protect their confidential information, that of their customers, trade secrets, their intellectual property, etc.
- 12. Governments should <u>support cybersecurity innovation through education and research and</u> <u>development (R&D)</u>:
 - Governments should support the development and generalization of cybersecurity curricula in university-level IT education.
 - Government support of cybersecurity R&D helps meet the future technological needs of each country's infrastructure, as well as help each country develops its IT industry.
 - Governments should support cybersecurity R&D through public funding of basic and long term research. They should limit their involvement in applied R&D to circumstances where the technological solution that is sought is not commercially available, and its absence creates a measurable security gap – thus focusing government resources on long-term need.
 - Governments should also consider creating incentives that encourage the private sector to conduct cybersecurity R&D.



BSA Worldwide Headquarters 1150 18th Street, N.W. Suite 700 Washington, DC 20036 USA Phone: +1.202.872.5500 Fax: +1.202.872.5501